DETAILED ACTION

1. In view of the Appeal Brief filed on 1/22/2007, PROSECUTION IS HEREBY REOPENED. The 102 rejection based on Yonge, III is withdrawn. However, after careful search, a new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

2. Claims 1-10 have been examined.

3. Any objections not repeated below for record are withdrawn.

Specification

4. The disclosure is objected to because: on page 1 of the specification, Applicant indicated "the HomePlug 1.01 Specification of the HomePlug Power Alliance, incorporated here by reference". First, the examiner noticed that the Applicant did **not** provide a copy of this reference to the office. Second, the Applicant **cannot** incorporate NPL reference into incorporated by reference. Please see 37 CFR 1.56,

1.57 and MPEP 201.17 for incorporation by reference. Therefore, the examiner will not consider "the HomePlug 1.01 Specification of the HomePlug Power Alliance" as incorporation by reference.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 4 - 6 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per **claim 4**, "...with the local NEK" is being recited. However, "the local NEK" lacks of antecedent basis. In the independent claim 1, "a unique, temporary NEK" is being recited. However, "local NEK" and "a unique, temporary NEK" are different keys.

As per **claim 6**, "...contains a unique, temporary NEK" is being recited. However, it is not clear whether this is the same as or different from "a unique, temporary NEK" recited in claim 1. Further, "confirming receipt of the temporary NEK...which is encrypted with the temporary NEK" is being recited. However, it is not clear whether this "the temporary NEK" referring to "unique, temporary NEK" in claim 1 or in the same claim. Furthermore, "using the determined MAC address to reliably send the local NEK" is being recited. First, "the local NEK" lacks of antecedent basis. Additionally, in the claim, "the local NEK" is being reliably sent, then why only "confirming receipt of the temporary NEK", not "the local NEK"?

Any claim not specifically addressed, above, is being rejecting as incorporating the deficiencies of a claim upon which it depends.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

9. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

10. Claims 1-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yonge, III (U.S. Patent 6,987,770) and in view of Chamberlain (U.S. Pub. No. 20030079000)

As per **claims 1 and 10,** Yonge, III discloses a method for determining MAC address for a remote device having a known, unique DEK in a network where devices may not send a confirmation to a SetNEK request, the method comprising the steps of:

preparing a broadcast message with a SetNEK request containing a unique, NEK (col. 33, lines 33-45);

encrypting the message with the DEK of the remote device ("The master station encrypts the frame using the received default key" – e.g. col. 33, lines 44-45 and step 594 in fig. 30. Please note default key corresponds to Applicant's DEK of the remote device);

transmitting the broadcast message ("transmits the encrypted frame to the new station…" – e.g. col. 33, lines 45-50 and step 596 in fig. 30) on a network medium (e.g. transmission medium 14 in fig. 3);

confirming receipt of the NEK by sending a request that requires a response from the remote device, wherein the request can be a request channel estimation MME and the response is a channel estimation response ("Referring to Figs. 13A – B…Referring to Fig. 13A, the Connection Information Request field 210 includes a Destination Address (DA) field 247. The DA specified by the DA field 247 is the address of the station for which the requesting station desires connection information. Referring to Fig. 13 B, the Connection Information Response Field 210D includes a DA field 248…Connection Information Request and Response are used for frame forwarding…" – e.g. col. 17, lines 42-61, "The master station may use the channel estimation function and channel estimation MAC management entries (Figs. 12 A and 12 B) described earlier to make the passing of the network encryption key to the new station more secure. The master station can send to the new station a channel estimation request, causing the new station to perform a channel estimation process. Upon receipt of this response, the master station utilizes the channel map specified in the response to send the encrypted frame (containing the NEK) to the new station" - e.g. col. 33, lines 51-62);

Yonge, III implicitly discloses the unique NEK can be a unique, temporary NEK by disclosing in col. 14, lines 35-45, "The Encryption Control field 180 includes an Encryption Key Select (EKS)

subfield 192...The 1-octet EKS field 192 **selects** either a default encryption/decryption key...**or one of 255 network keys**...the selected key to encrypt/decrypt the frame data" and in col. 34, lines 1-10 "The value of the Encryption Key Select 604 is placed in the EKS field 192 of the frame in **all** transmissions between members of the logical network...".

Yonge, III does not expressly disclose the unique NEK is a unique, temporary NEK, the request is encrypted with the temporary NEK.

In the same field of endeavor of powerline network (e.g. par. [0005] of Chamberlain), Chamberlain et al. discloses using a unique, temporary NEK (i.e. one-time encryption key), the request is encrypted with the temporary NEK ("...a security system 502, is added to the new secure logical network 406 of fig. 4. The secure device 502 differs from other smart devices...in the arrangement at least in that the smart device is designed to respond only to configuration messages that are encrypted with a **"one-time" encryption key**...**sufficiently randomized**...The phrase "**one-time**" is used to **distinguish this encryption key from the network encryption key** described above. The encryption key associated with the secure device 502 is used only when the device 502 is participating in a configuration session. This key is to be **contrasted** with the network encryption key which may be used to encrypt every message exchanged between devices of a given logical network. Thus, the key will be **used only one time**...using this one-time encryption key, the secure device 502 and the secure NCA 402 may exchange secure configuration messages over the shared bus 102 during a configuration session. Thus, only the secure NCA 402 will be capable of responding to requests for configuration received from the secure device 502 that are encrypted with the one-time key. Similarly, only the secure device 502 will be capable of responding to

solicitations received from the secure NCA 402 that are encrypted with the one-time key. " – e.g. par. [0049] – [0051])

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate using a unique, temporary NEK (i.e. one-time encryption key), the request is encrypted with the temporary NEK of Chamberlain et al. into Yonge III in order to prevent the newly added device from being captured into an incorrect logical network and further prevent the network encryption key from being acquired by unauthorized devices during any configuration session that takes place between the newly added device and already established logical network, to easily add new or additional devices to the home and to configure these devices to join an already established logical network with a minimum of interaction and skill from the homeowner and to support the secure exchange of messages over the shared bus (e.g. Chamberlain et al. par. [0015], [0051] – [0052] and par. [0060])

Yonge, III – Chamberlain further discloses determining the MAC address of the remote device from the response (Yonge, III, "In response to these inputs, it provides…new station address" –e.g. col. 26, lines 44-61, col. 1, lines 40-45, "…a Destination Address (DA) 108…Each address is an IEEE 48-bit MAC address format" – e.g. col. 10, lines 4-9, "upon receipt of this response, the master station utilizes the channel map specified in the response to send the encrypted frame (containing the NEK) to the new station" –e.g. col. 33, lines 59-61 and "Referring to Figs. 13A – B…Referring to Fig. 13A, the Connection Information Request field 210 includes a Destination Address (DA) field 247. The DA specified by the DA field 247 is the address of the station for which the requesting station desires connection information. Referring to Fig. 13 B, the Connection Information Response Field 210D includes a DA field 248…Connection Information Request and

Response are used for frame forwarding..." – e.g. col. 17, lines 42-61. Please note the response by returning a frame includes Connection Information Response MAC management entry 210 D (from Fig. 13B) and in which the remote device address is included and being determined; "encrypt physical address ...with one-time key" in step 616, fig. 6 and "send unique physical address to device" in step 618, fig. 6 in Chamberlain. Chamberlain further discloses in par. [0060], "...Applicant acknowledges that many of the hardware devices designed to operate over these media, especially those designed to operate over wireless media, have hardware identifiers (or addresses) pre-assigned to them by manufacturers. Unique hardware addresses are pre-assigned based on the various communication protocols used...the devices may be addressed within the logical network using their pre-assigned address." Please note unique hardware identifier is device's MAC address and the network encryption key is sent to the device after device's address is determined from the request/response between the device and the NCA in fig. 6. Further, it is common knowledge to a person with ordinary skill in the art that the physical address (i.e. MAC address) of the remote device must be determined before the sender (i.e. NCA) is able to send information (i.e. the network encryption key) to the device.

As per **claim 2**, Yonge, III – Chamberlain discloses a method as applied in claim 1. Yong, III - Chamberlain further discloses wherein the remote device is not a member of a network (Yonge, III, new station 12e in fig. 29 and col. 33, lines 1-12 and 33-34 and Chamberlain, "Accordingly, there also exists a need for techniques to easily add new or additional smart devices to the home and to configure these devices to join an already established logical network with a minimum of interaction and skill from the homeowner. The techniques should be such that newly or additionally installed devices should be configurable to not interfere with the operation of existing household wiring or to override existing wired

connections if the homeowner so desires." – e.g. par. [0011] and [0015]. Please note new or additional smart devices corresponds to Applicant's remote device).

As per **claim 3**, Yonge, III – Chamberlain et al. discloses a method as applied in claim 2. Yonge, III – Chamberlain further discloses comprising the step of using the MAC address of the remote device in a unicast transmission to reliably confirm receipt of the temporary NEK (e.g. Yonge, III, col. 11, line 43 and col. 44, line 59-67).

As per **claim 4**, Yonge, III – Chamberlain et al. discloses a method as applied in claim 3. Yonge, III – Chamberlain further discloses comprising the step of using the MAC address of the remote device in a unicast transmission (Yonge, III, "unicast transmission"- e.g. col. 10, lines 39-40) containing a SetNEK message with the local NEK (Yonge, III, col. 34, lines 11-26 and step 620 in fig. 6 of Chamberlain et al.).

As per **claim 5**, Yonge, III – Chamberlain et al. discloses a method as applied in claim 4. Yonge, III further discloses comprising the step of using the MAC address of the remote device in an additional unicast transmission which is encrypted with the local NEK, for purposes of confirming receipt of the local NEK (col. 11, line 43).

As per **claim 6**, Yonge, III – Chamberlain et al. discloses a method as applied in claim 2. Yonge, III further discloses using the determined MAC address to reliably send the local NEK (col. 33, lines 59-62); preparing a unicast message to the remote device containing a SetNEK request where the SetNEK request contains a unique, temporary NEK (col. 33, lines 38-45); encrypting the unicast message with the DEK of the remote device ("The master station encrypts the frame using the received default key" – e.g. col. 33, lines 44-45 and step 594 in fig. 30); transmitting the unicast message on the medium ("transmits the encrypted frame to the new station…" – e.g. col. 33, lines

45-50, fig. 29 and step 596 in fig. 30); and confirming receipt of the temporary NEK by sending a request that requires a response which is encrypted with the temporary NEK (col. 33, lines 51-59).

As per **claim 7**, Yonge, III – Chamberlain et al. discloses a method as applied in claim 1. Yonge, III - Chamberlain further discloses wherein the network is a powerline network (Yonge, III, col. 6, lines 22-24 and fig. 1; Chamberlain, "...powerline carrier (PLC), which uses AC power lines..." – e.g. par. [0005] and fig. 1).

As per **claim 8**, Yonge, III – Chamberlain et al. discloses a method as applied in claim 1. Yonge, III further discloses wherein the remote devices are implemented according to the HomePlug Powerline Alliance standard (on page 3, Yonge, III cited "HomePlug Powerline Alliance, HomePlug 1.0.1 Specification, Dec. 1, 2001).

As per **claim 9**, Yonge, III – Chamberlain et al. discloses a method as applied in claim 1. Yonge, III further discloses wherein the request is a request statistics MME and the response is a statistic response MME (col. 15, Table 2 "Request parameters and statistics" and "Parameters and Statistics Response" and col. 18, lines 65-col. 19, line 3).

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure (See PTO -892).

Applicant is **strongly urged** to review these references in response to the current office action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to APRIL Y. SHAN whose telephone number is (571)270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/April Y Shan/
Examiner, Art Unit 2135
/KIMYEN VU/
Supervisory Patent Examiner, Art Unit 2135